ILLEG

OGC 79-00197

8 January 1979

MEMORANDUM FOR: Chairman, DCI Security Committee
Chief, Policy and Coordination Staff/DDO
Special Assistant/DDS&T

STATINTL FROM: [redacted]
Assistant General Counsel

SUBJECT: HPSCI Hearings on the Protection and Use of National Security Information in Criminal and Civil Litigation

1. Chairman Boland's letter to the DCI advising of the subject hearings is at Tab A and includes a hearing schedule and tentative witness list and "prospectus" which outlines the Committee's objectives. The General Counsel has been designated to appear on the DCI's behalf with the understanding that he can call upon other components and individuals for assistance as needed (Tab B).

2. At present, it appears that your assistance may be needed in connection with the session scheduled for 1 February 1979 (see tentative schedule and prospectus). At the morning session that day, the Committee intends to examine cases of intelligence disclosures that were not investigated or prosecuted. We may be called upon to explain why the disclosures were damaging and any factors which weighed against investigative or prosecutive action. In the afternoon session we will be asked to suggest categories of secrets the disclosure of which might warrant treatment as separate criminal offenses without regard to existing law. We should have further guidance after we discuss the hearings with members of the HPSCI Staff on 11 January.

[redacted] STATIN

STATINTL Attachments

cc: [redacted] OLC
Special
Security Center

All Portions of This
Document are Unclassified.

OS 9 0076

H-405, U.S. CAPITOL
(202) 225-4121

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

WASHINGTON, D.C. 20515

December 22, 1978

Honorable Stansfield Turner
Director of Central Intelligence
Washington, D. C. 20505

Dear Admiral Turner:

The Permanent Select Committee on Intelligence intends to hold a series of hearings beginning in late January 1979 concerned with the protection and use of national security information in the context of both criminal and civil litigation. The hearings, which will consist of seven sessions spanning four days, will concentrate on the problems inherent in trying cases involving espionage, leaks of classified material, and the phenomenon called "graymail" as well as the use of pre-publication review and other civil proceedings to preclude the publication of classified material. The hearings will be conducted by the Subcommittee on Legislation, chaired by Congressman Morgan F. Murphy.

Because of your great interest in this subject, both as the Director of Central Intelligence and head of the Central Intelligence Agency, I am proposing that you designate witnesses to appear on your behalf to discuss various problems that the intelligence community has encountered in the areas within the scope of the Committee's inquiry. I believe, on the basis of previous appearances before this Committee, that your General Counsel, Anthony Lapham, has an excellent grasp on the issues that will arise in the context of the Committee's hearings and would be a fine lead-off witness.

As an aid to preparation for participation in the hearings, I enclose a prospectus for each session, materials which embody some suggested remedies to the problems of litigation involving national security information and a tentative witness list. To assist the Committee staff in preparing for the hearings, it would be appreciated that any written statement be submitted at least 72 hours in advance. Additional information concerning the hearings may be obtained from Mr. Michael O'Neil, Chief Counsel of the Committee, at 225-4121.

With every good wish, I am

Sincerely yours,

Edward P. Boland

EDWARD P. BOLAND
Chairman

Enclosures

HEARING SCHEDULE
WITH TENTATIVE WITNESS LIST

All Hearings will be held in Room H-405 in the Capitol Building.

January 24

Morning Session:	9:00 a.m.-12:00 noon (open)
Topic:	The Problem
Witnesses:	Robert Keuch, Deputy Assistant Attorney General for Criminal Division
	Anthony Lapham, General Counsel, CIA
STATINTL	[redacted] General Counsel, CIA
Afternoon Session:	1:00-4:00 p.m. (open)
Topic:	Pre-Publication Review
Witnesses:	Anthony Lapham, General Counsel, CIA
	Representative from Department of Justice, Civil Division
	Mark Lynch, ACLU Attorney

January 25

Morning Session	9:00 a.m.-12:00 noon (open)
Topic:	Proposals
Witnesses:	Senator Joseph Biden, Chairman, Subcommittee on Secrecy and Disclosure, Senate Select Committee on Intelligence
	Philip Lacovara, Esq., Hughes, Hubbard and Reed
	Professors Harold Edgar and Benno C. Schmidt, Jr., Columbia Univesity Law School

January 31

Morning Session:	9:00 a.m.-12:00 noon (open)
Topic:	Comment on Legislative Proposals by Distinguished Legal Scholars
Witnesses:	William Colby, Colby, Miller and Hanes
	Edward Levi, University of Chicago Law School
	Antonin Scalia, University of Chicago Law School
Afternoon Session:	1:00-4:00 p.m. (open)
Topic:	Comment on Legislative Proposals by Distinguished Civilian Trial Lawyers
Witnesses:	Mitchell Rogovin, Rogovin, Stern and Huge
	William Hudley, Attorney at Law
	Michael Tigar, Tigar and Baffome

February 1

Morning Session:	9:00 a.m.-12:00 noon (closed)
Topic:	Case Histories of Intelligence Disclosures Which Were Not Investigated or Prosecuted
Witnesses:	Representatives of CIA, NSA, DoD and DoJ
Afternoon Session:	1:00-4:00 p.m. (closed)
Topic:	Genuine National Security Secrets
Witnesses:	Representatives of CIA, NSA, DoD and DoJ

Bibliographic Note

During the course of the hearings, attention will be given to certain proposals advanced by experienced commentators on how to resolve perceived problems in the use and protection of national security information through both civil and criminal litigation. For purposes of reference the conclusions of Professors Schmidt and Edgar may be found in the enclosed portion of their landmark review of the espionage statutes. The complete work, entitled "The Espionage Statutes and Publication of Defense Information" may be found at 73 Columbia Law Review 929 (May 1973). It is strongly recommended as the most authoritative work of its kind.

Also included in the materials under this cover are the 1978 report and hearings of the Senate Select Committee on Intelligence's Subcommittee on Secrecy and Disclosure. The Subcommittee, chaired by Senator Joseph R. Biden, explored the same subjects which this Committee hopes to consider. Among the witnesses to appear before the Subcommittee were Mr. Phillip Lacovara, former Deputy Solicitor General and counsel to the Watergate Special Prosecutor and Mr. William Colby, former Director of Central Intelligence. Both gentlemen advanced suggestions in the course of their testimony (Beginning respectively on pages 59 and 89 of the hearings) which the hearings will address directly.

Finally, the hearings will solicit understanding of, and comment on, the recommendations contained in the Subcommittee's report (beginning on page 30 of the report).

Examination of all these materials should aid witnesses in focusing on current thinking about the espionage statutes and related issues. The Committee wishes to solicit comment on these proposals and any others which witnesses may wish to make - as well as references to other materials of which the Committee is unaware.

PROSPECTUS

On January 24, 1979, the Legislative Subcommittee of the House Permanent Select Committee on Intelligence will begin four days of hearings devoted to the constitutional, legal, and intelligence problems involved in utilizing civil litigation or the criminal justice system to protect classified information against unauthorized disclosure.

Such disclosures may be effected in a variety of ways -- clandestine transmittal to a foreign government by an espionage agent, leaks to the press by a former government employee, or testimony during trial by a criminal defendant or a witness on his behalf -- all of which may equally threaten the national security. However, the government's response to such disclosures has varied from forceful prosecution to active disregard. To the extent that such disparate treatment and any detrimental result are caused by attention to constitutional principles there may be no solution to the core problem. However, to the extent that a failure to adequately prevent or respond to disclosures of classified information is caused by poorly drafted legislation, a lack of legislation, restrictive or conflicting judicial procedures, intra-executive branch squabbling, institutional myopia, or the abuse of prosecutorial discretion, a solution may be reachable and necessary.

Some suggest that the root of the problem lies with the existing espionage laws, which are not tied to the classification system and which, because they require proof of intent to harm the United States or advantage a foreign nation and of the relation of the information or document to the national defense, necessitate making public the very information, the transfer or disclosure of which is the reason for the prosecution. In addition, considerable doubt has been expressed as to whether the scope of the espionage laws was ever intended to extend beyond real espionage to the common "leak"-- especially when the leak is published in book form. Finally, while 18 U.S.C. 798 purports to make the unauthorized disclosure of classified cryptologic and communications security information a per se offense, there is a legitimate question whether the judge or the jury, or both, have the duty to look behind the classification to determine if the information disclosed was properly classified.

In addition to the problems inherent in the espionage statutes, the Federal Rules of Criminal Procedure and related concepts require the disclosure of a great amount of information during the normal course of a criminal trial. Any effort to restrict the defense's access to relevant information threatens to make the judge a trier of fact,

while the conduct of portions of a criminal trial behind closed doors may endanger cherished constitutional principles. In the same manner, proposals to make the unauthorized disclosure and/or retention of classified information a criminal offense have substantial first amendment implications -- which are compounded by the abuse and misuse to which the existing classification system is subject.

The above are some of the factors that appear to the Committee to complicate consideration of the protection and use of national security information through litigation. The hearings will concentrate on these and related issues. They will attempt to determine if problems really exist and, if so, what can or should be done about them. To the extent possible, the discussion of the issues will be channeled into four separate areas: espionage, leaks, pre-publication review, and "graymail". To that end, the following synopses of the seven sessions of the hearings are intended to focus on what, at the outset, the Committee hopes to explore at each session.

First Session

January 24, 1979 - Morning

This session will be devoted to an explication of the problem as perceived by the Department of Justice, the CIA, and the NSA. Lawyers from these agencies will be asked to summarize their view of the content and scope of the espionage laws and the extent to which these laws aid or hinder the prosecution of espionage and leak cases, and, as a result, either aid or hinder the protection of classified information.

Drawing on their practical experience, the witnesses will be asked to describe those elements of constitutional law or criminal procedure which, in their view, require or allow the disclosure of classified information during a prosecution, depending on whether the disclosure is made by the government or the defendant, and whether the defendant is a spy, a leaker, a government employee accused of other wrongdoing, or a nongoverment employee charged with crimes unrelated to espionage or leaks.

Testimony will also be elicited as to the manner in which intelligence agencies and the Department of Justice determine whether an espionage or leak case is to be investigated and prosecuted, and as to the existence of any institutional conflicts which hinder this determination.

Apparently, many such cases have gone uninvestigated and/or unprosecuted because the intelligence agencies hesitate to disclose the classified information necessary for trial, while the Justice Department refuses to even begin an investigation until the intelligence agencies agree to such a declassification.

The witnesses also will be asked to comment on whether even a strong anti-leak law would lead to prosecution of the high government officials who some perceive to be the source of most important leaks, or whether such a law would be otherwise utilized in light of the oft-stated concern that to prosecute - or even investigate - a leak would only further publicize or confirm the accuracy of its content.

In summary, the first session should explicate any existing problems, attempt to determine to what degree they are caused by a lack of effective criminal statutes or the strictures of the criminal trial process, institutional prejudices and/or conflicts, or a lack of prosecutorial initiative, so as to aid the Committee in assessing recommendations on corrective legislation or administrative action.

Second Session

January 24, 1979 - Afternoon

The second session will concentrate on the leak/espionage problem as it relates to disclosure of classified information by way of publication in print, and the attendant and difficult issues of pre-publication review and/or restraint and post-publication remedies.

Department of Justice and CIA witnesses will be asked to describe the Government's legal response (or lack thereof) to such cases in the past (Marchetti/Marks, Agee, Snepp, Stockwell), with some detail expected as to the legal theories involved, judicial rulings thereon, and the various alternative actions that may have been discussed but not taken. Recommendations as to remedies will be sought and comments solicited on existing proposals to criminalize the publication of names of intelligence agents.

Other witnesses presenting the viewpoint of previous defendants in pre-publication suits will be asked to respond to the preceeding testimony and comment on legislative proposals.

It is expected that all witnesses will discuss such topics as secrecy oaths and agreements, injunctive relief (whether or not based on contract theories), criminal and civil penalties, and pre-publication review by intelligence agencies. Particular attention should be paid to the judicial theories propounded in the New York Times, Marchetti, and Snepp cases.

Third Session

January 25, 1979 - Morning

This session will hear from Professors Schmidt and Edgar, Senator Biden, and former Assistant Special Prosecutor Lacovara -- all of whom have previously studied and/or testified on subjects relating to espionage laws and leaks. (Former Director of Central Intelligence Colby has also advanced a proposal in this context, but will be unable to appear until the January 31 morning session.) They will be asked to state any problems they perceive in the espionage/leak area, comment on suggested remedies, and offer their solutions -- all in the context of their particular area of expertise.

The attached report of the Subcommittee on Secrecy and Disclosure of the Senate Select Committee on Intelligence contains Senator Biden's recommendations. The accompanying hearings contain the views of William Colby and Phillip Lacovara. Also attached are the recommendations with which Professors Schmidt and Edgar concluded their seminal 1973 Columbia Law Review article on the espionage laws. Some of the suggestions of these and other students of the issue include:

* Prospectively defining a list of super secrets (which may or may not include sources and methods) separate

from the existing classification system, the unauthorized disclosure of which would be a per se criminal offense;

* Rewriting the espionage laws so as to make the unauthorized disclosure of classified information to a foreign government or agent a per se criminal offense;

* Defining an evidentiary state secrets privilege available to the government when the defense seeks access to classified information, with the determination as to its proper invocation and applicability to be made by the judge in camera, coupled with a sliding scale of remedies for non-disclosure available to the defense at the judge's discretion.

* Make the unauthorized disclosure of any classified information a criminal offense, but exempt the recipient of the information from liability, require that a government agency be established to hear classification appeals before a prosecution could be initiated, and make it an affirmative defense, to be decided by the judge in camera, that the information was not properly classified.

* Establishing special pre-trial procedures for cases where national security secrets are likely to arise in the course of a prosecution which would require the defendant to put the government on notice of all motions, defenses, or arguments he intended to make which would require the discovery or disclosure of classified information or the use of intelligence community witnesses. The court would

then be required to rule in advance on the admissability and relevance of the information and on the scope of witnesses' testimony.

* Make it a criminal offense for a government employee or former employee to disclose classified information without first giving notice to the relevant agency and waiting a specified period of time; during the waiting period the government would be required to review the classification and, if it were determined that the classification was proper, could seek an injunction under the Pentagon Papers standard; absent an injunction, no criminal penalty would attach to disclosure at the end of the waiting period - even if the information had been determined to be properly classified; per se criminality would attach, however, to any government employee and former employee who discloses classified information without going through this process.

Fourth and Fifth Sessions

January 31, 1979 - Morning - Afternoon

These sessions will hear from distinguished legal scholars and practioners with expertise in criminal law and procedure and the constitutional and legal issues related thereto.

These witnesses will be asked to comment on the practicality, propriety, and constitutionality of the various proposals mentioned hereinabove, to detail some of the problems involved in defending a criminal case, and delineate the manner in which some of the proposals might impinge on a defendant's rights. Specific attention should be directed to:

(1) the content of the sixth amendment's guarantee of a public trial;

(2) the sixth amendment implications of the application of a protective order to the defendant and his counsel;

(3) the criteria for distinguishing between an issue of fact to be decided by the jury and an issue of law to be decided by the judge;

(4) the due process/fair trial implications of a state security privilege and a requirement that the defense give pre-trial notice of its arguments, motions, and defenses;

(5) the due process/fair trial implications of a statute which would make disclosure of intelligence sources and methods

a per se offense, and allow the judge to determine in camera whether the disclosed information dealt with sources and methods.

The views of the witnesses will also be sought on the first amendment issues involved in:

(1) pre-publication review/post-publication penalties proposals, and

(2) criminal penalties for disclosure or reception of any classified information.

Sixth and Seventh Sessions

February 1, 1979 - Morning and Afternoon

The morning session will be closed to the public. Intelligence agency and Department of Justice officials will discuss actual cases of espionage or damaging leaks which were prosecuted and those which were not; define actual damage to the national security caused by the leaks; and explain why there was no investigation and/or prosecution in some cases. It is hoped that this session will serve to draw out examples of the actual workings of present practice, its drawbacks and how porposed changes would affect future cases.

The afternoon session will also be closed. Intelligence agency officials will be asked to define those secrets which should be placed in a special category separate from the existing classification system, the unauthorized disclosure of which would be serious enough to warrant designating disclosure of such as a per se criminal offense.

mention them briefly here to complete our overview of other statutes governing particular areas of information relating to the national security.

VIII. Conclusion: Room for Improvement

The basic espionage statutes are totally inadequate. Even in their treatment of outright spying they are poorly conceived and clumsily drafted. The gathering and obtaining offenses of subsections 793(a) and 793(b) have no underlying purpose that could not be served by more precise definition of attempts to violate the transmission offenses of subsection 794(a). No subsection of the general provisions of sections 793 or 794 has an easily understood culpability standard. Subsections 794(a), 793(a) and 793(b) employ "intent or reason to believe information is to be used to the injury of the United States or to the advantage of any foreign nation." Surely, however, Congress did not wish to subject negligent conduct to the death penalty by using the words "reason to believe"; nor is it clear what is meant by "is to be used" or "advantage" and "injury."

Subsection 793(c) is another puzzle. The culpability required turns on the meaning of the phrase "for the purpose aforesaid." The two sections immediately preceding it, subsections 793(a) and (b), state that conduct done "for the purpose of" obtaining information respecting the national defense, and with intent or reason to believe, is criminal. In light of the prior use of "purpose" and "intent" as separate requirements, the common-sense reading of subsection 793(c) is that "for the purpose aforesaid" means only "for the purpose of obtaining national defense information" and not "intent and reason to believe." Yet all the evidence we have found indicates agreement by both Congress and the Executive Branch that subsection 793(c) requires the same culpability as subsections 793(a) and (b).

Then, there are the mysteries of the term "willfully" in subsections 793 (d) and (e) and the added twist that a special "reason to believe" culpability requirement that allegedly protects in special fashion those who disclose "information," but not documents, is itself a problematic distinction. The phrase adds content to the law, however, only if the rest of the statute is read so broadly as to be clearly unconstitutional. Finally, there is 794(b)'s intent standard, which can be given a clear interpretation—intent means conscious purpose—only by making the statute paradoxical. Why did Congress choose to subject publications to controls pursuant to a standard that so rarely will be met? Why should actions taken by publications with the purpose of furthering foreign interests by disclosing national defense secrets not be criminal except in time of war? In light of this confusion about culpability, [illegible] it is somewhat ironic to recall the confident assertions in *Gorin* that the vague parameters of "national defense information" may be ignored because scienter is required.

The difficulty in finding the proper application of the laws to clandestine espionage is minor compared to the incredible confusion surrounding the issue of criminal responsibility for collection, retention, and public disclosure of defense secrets. In essence, a choice must be made between giving effect either to broad statutory language designed in the Executive Branch or to the considerable evidence spread over a half-century that Congress wanted much more limited prohibitions. The choice is particularly difficult since the evidence of congressional intent is not absolutely clear. Issues were not precisely understood by lawmakers who were often unenlightened and at cross-purposes with one another over the meaning of basic terms. Nevertheless, on the issue of the criminality of public debate, one proposition is, in our view, unquestionable: neither the Congresses that wrote the laws nor the Executives who enforced them have behaved in a manner consistent with the belief that the general espionage statutes forbid acts of publication or conduct leading up to them, in the absence of additional and rarely present bad motives.

Regardless of the proper construction of the current statutes, it is time for clarification by legislation that treats the problem anew. The ambiguity of the current law is tolerable only because the limits of the right to disclose and publish have been so rarely tested. This pressing to the limits is, in a sense, the deeper significance of the publication of the Pentagon Papers. It symbolizes the passing of an era in which newsmen could be counted upon to work within reasonably well understood boundaries in disclosing information that politicians deemed sensitive. As remarkable as the constant flow of leaked information from the Executive Branch since the classification programs were implemented[413] is the general discretion with which secret information has been used[414] (attesting to the naturally symbiotic relationship between politicians and the press). The New York Times, by publishing the Papers, did not merely reveal a policy debate within the Executive Branch; it demonstrated that much of the press was no longer willing to be merely an occasionally critical associate devoted to common aims, but intended to become an adversary threatening to discredit not only political dogma but also the motives of the nation's leaders. And if the Times should be discreet, some underground newspaper stands ready to publish anything that the Times deems too sensitive to reveal.[416]

413. *See* The New York Times Company v. United States: A Documentary History 397 (Comp. by J. Goodale, 1971) (affidavit of Max Frankel) (1971).

414. The most famous recent case is the New York Times' decision not to report the upcoming Bay of Pigs venture. S. Ungar, The Papers and the Papers 101-02 (1972). More significant perhaps, the United States fought World War II without any official censorship of the press.

415. [illegible] claims that the United States has had remarkable success in breaking the codes of the U.S.S.R., a matter of great importance if true. *See U.S. Electronic Espionage: A Memoir*, Ramparts, August, 1972, at 35.

This changing role of the press is a necessary counterweight to the increasing concentration of the power of government in the hands of the Executive Branch. There are, however, aspects to the development that are troublesome in the context of national defense secrets. We reject the utopian notion that there are no defense secrets worth keeping and that every aspect of national security should be disclosed to facilitate adequate public comprehension of the policy choices to be made. Yet technology makes document copying ever more simple. As the lower levels of the executive bureaucracy, shut off from real participation in decision-making, are racked by the same conflicts about the ends and means of foreign policy that characterize the wider community, criminal sanctions assume greater significance in the protection of the Government's legitimate secrecy interests. Paradoxically, the likely consequence of the law's failure to give weight to security considerations would be to augment the strong tendency to centralize power into fewer hands, because only a small group can be trusted to be discreet.

If regulation of publication is necessary, it is far better for Congress to do the job than to permit the Executive Branch to enforce secrecy by seeking injunctive relief premised upon employee breach of adhesion contracts. In the recent *Marchetti* case,[416] a former C.I.A. agent was enjoined from publishing, without prior agency approval, accounts of his experience as an intelligence agent.[417] He had signed an agreement as a condition of employment saying that he would never reveal "information related to the national defense."[418] Although the policy of requiring government officials, past and present, to remain silent may be wise, it is not a question that ought to be relegated to judicial enforcement of executive contracts, thereby excluding from policy formation the one branch most entitled to decide. Only the fact that the Government will so rarely have advance notice of intent to publish keeps the *Marchetti* precedent for injunctive relief from becoming a dangerous alternative to the necessity of legislative clarification.

The opportunity for careful reevaluation of the espionage problem is at hand, since Congress is now considering the recodification and reformulation of the federal criminal law. Few undertakings deserve greater support. The present federal criminal law suffers generally from the confusion and defects that inevitably occur when major problems in the law of crimes requiring conceptual clarity and overall design are left to the ad hoc responses of successive Congresses.[419] But revision is a task of awesome complexity, particularly as to matters like espionage where the underlying problems have not been explored in the course of recent efforts to revise state criminal codes. Unfortunately, the espionage proposals currently before Congress as part of S. 1[420] and S. 1400,[421] the Nixon Administration's latest proposal, are inadequate to reconcile the conflicting interests at stake. Insofar as there have been five different espionage proposals[422] in the last two years, and there are surely more to come, general discussion of the approach of the two most recent revision proposals seems more appropriate than detailed analysis.

The basic problem with S. 1 is that too much of the sloppy drafting of the old law is perpetuated and the new formulations do not resolve the problems that perplexed former Congresses. S. 1 treats the matters now covered by sections 793-98 with the following provisions:

> § 2-5B7. Espionage
>
> (a) OFFENSE.—A person is guilty of espionage if:
>
> (1) with knowledge that the information is to be used to the injury of the United States or to the advantage of a foreign power, he gathers, obtains, or reveals national defense information for or to a foreign power or an agent of such power; or
>
> (2) with intent that it be communicated to the enemy and in time of war, he elicits, collects, records, publishes, or otherwise communicates national defense information.
>
> (b) ATTEMPT.—Without otherwise limiting the applicability of section 1-2A4 (criminal attempt), any of the following is sufficient to constitute a substantial step under such section toward commission of espionage under subsection (a)(1): obtaining, collecting, or

416. United States v. Marchetti, 466 F.2d 1309 (4th Cir.), *cert. denied*, 93 S. Ct. 553 (1972).

417. The Court held that the C.I.A. might disapprove publication only of matters that were both classified and had not been publicly disclosed. But "rumor and speculation are not the equivalent of prior disclosure. . . ." 466 F.2d at 1318. Opportunity for judicial review of the propriety of classification was denied. *Id.*

418. 466 F.2d at 1312. The agreement stated, in part:

> 1. I, Victor L. Marchetti, understand that by virtue of my duties in the Central Intelligence Agency, I may be or have been the recipient of information and intelligence which concerns the present and future security of the United States. This information and intelligence, together with the methods of collecting and handling it, are classified according to security standards set by the United States Government. I have read and understand the provisions of the espionage laws, Act of June 25, 1948, as amended, concerning the disclosure of information relating to the National Defense and I am familiar with the penalties provided for violation thereof.
>
> 2. I acknowledge, that I do not now, nor shall I ever possess any right, interest, title or claim, in or to any of the information or intelligence or any method of collecting or handling it, which has come or shall come to my attention by virtue of my connection with the Central Intelligence Agency, but shall always recognize the property right of the United States of America, in and to such matters.

The agreement does not reflect current law on either our, or apparently the C.I.A.'s, The agreement does not reflect current law on either our, or apparently the C.I.A.'s, reading of it. See Memorandum of the Central Intelligence Agency entitled "The

419. *Cf.* Wechsler, *The Challenge of a Model Penal Code*, 65 HARV. L. REV. 1097 (1952).

420. S. 1, 93d Cong., 1st Sess. §§ 2-5A1, 2-5B7-8 (1973). The bill, reputedly the lengthiest ever introduced, is derived, with substantial changes, from the FINAL REPORT OF THE NATIONAL COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, PROPOSED NEW FEDERAL CRIMINAL CODE (1971).

421. S. 1400, 93d Cong., 1st Sess. §§ 1121-26 (1973).

422. S. 1 and S. 1400, see §§ 2-5B7-8 in the Committee Print leading to S. 1, the FINAL REPORT OF THE NATIONAL COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, PROPOSED NEW FEDERAL CRIMINAL CODE, §§ 1112-1116 (1971) and the COMMISSION'S STUDY DRAFT OF A NEW FEDERAL CRIMINAL CODE §§ 1113-6

eliciting national defense information, or entering a restricted area to obtain such information.

(c) GRADING.—The offense is a Class A felony if committed in time of war or if the information directly concerns military missiles, space vessels, satellites, nuclear weaponry, early warning systems or other means of defense or retaliation against attack by a foreign power, war plans, or defense strategy. Otherwise it is a Class B felony.

§ 2-5B8. Misuse of National Defense Information

(a) OFFENSE.—A person is guilty of an offense if in a manner harmful to the safety of the United States he:

(1) knowingly reveals national defense information to a person who is not authorized to receive it;

(2) is a public servant and with criminal negligence violates a known duty as to custody, care, or disposition of national defense information, or as to reporting an unauthorized removal, delivery, loss, destruction, or compromise of such information;

(3) knowingly having unauthorized possession of a document or thing containing national defense information, fails to deliver it on demand to a Federal public servant entitled to receive it;

(4) knowingly communicates, uses, or otherwise makes available to an unauthorized person communications information;

(5) knowingly uses communications information; or

(6) knowingly communicates national defense information to an agent or representative of a foreign power or to an officer or member of an organization which is, in fact, defined in section 782(5), title 50, United States Code.

(b) GRADING.—The offense is a Class C felony if it is committed in time of war. Otherwise it is a Class D felony.

The key term "national defense information" is explicitly defined:

"[N]ational defense information" means information regarding:

(i) the military capability of the United States or of a nation at war with a nation with which the United States is at war;

(ii) military or defense planning or operations of the United States;

(iii) military communications, research, or development of the United States;

(iv) restricted data as defined in section 2014, title 42, United States Code;

(v) communications information;

(vi) in time of war, any other information which if revealed could be harmful to national defense and which might be useful to the enemy;

(vii) defense intelligence of the United States, including information relating to intelligence operations, activities, plans, estimates, analyses, sources, and methods.

In our opinion, enactment of this proposal would do no more than perpetuate the current confused state of the law. Consider the espionage

offenses of section 2-5B7, which for the most part restates the current section 794. Like subsections 794(a) and (b), the two offenses created are nearly identical. Section (a)(1) makes knowledge that national defense information "is to be used" to the injury of the United States or to the advantage of a foreign nation the test of whether a crime is committed. Does one who publishes "reveal . . . for or to a foreign power" within the meaning of the law? If not, it is only because 2-5B7(a)(2) says "publishes" while (a)(1) does not. Whatever the proper resolution, it is a mistake for recodification to treat such an important issue so opaquely. Similarly, publishing is explicitly made criminal only in time of war and only where there is "intent that [the information] be communicated to the enemy." The proposed code defines "intentionally" to require a conscious objective to cause the particular result.[423] Consequently, as in 794(b), the purported coverage of publication is largely illusory because very few newspapers intend to inform the enemy.

The new offense of "Misuse of National Defense Information" in section 2-5B8 is also perplexing, although we can be thankful that it departs from the models set out by section 793, particularly in its dispatching with the entitlement concept. Is publishing or conduct incident thereto meant to be covered? What is the meaning of "in a manner harmful to the safety of the United States?" Aside from issues of vagueness, is this phrase intended to require that the prosecutor prove that because of the actor's conduct consequences harmful to United States' safety actually resulted, were likely to result or might conceivably have come about?[424] To ignore clear resolution of these issues is to be satisfied with a statute whose basic design defies interpretation.

The Administration's proposals in S. 1400 do not suffer from these ambiguities. Their problem is that they are so excessively restrictive of public debate that their unconstitutionality, let alone their misconceptions of appropriate public policy, is, in our view, patent. Five offenses, too lengthy to be fully set out, are defined: espionage,[425] disclosing national defense information,[426] mishandling national defense information,[427] disclosing classified information,[428] and unlawfully obtaining classified information.[429] The proposed espionage offense is drafted with remarkable breadth:

(a) OFFENSE.—A person is guilty of an offense, if, with intent that information relating to the national defense be used, or with knowledge that it may be used, to the prejudice of the safety or interest

423. S. 1, 93d Cong., 1st Sess. § 1-2A1(a)(2) (1973).

424. Whether the statute is intended to achieve the results it does is problematic. Note for example, that it would repeal section 793(e)'s retention offense. In addition, the treatment of communications information, earlier defined as "national defense information" is either redundant or hopelessly opaque.

425. S. 1400, 93d Cong., 1st Sess. § 1121 (1971).

427. *Id.* at § 1123.

428. *Id.* at § 1124.

429. *Id.* at § 1125.

of the United States, or to the advantage of a foreign power, he knowingly:

(1) communicates such information to a foreign power;
(2) obtains or collects such information for a foreign power or with knowledge that it may be communicated to a foreign power; or
(3) enters a restricted area with intent to obtain or collect such information for a foreign power or with knowledge that it may be communicated to a foreign power.

Insofar as "communicate" means "to make information available by any means, to a person or to the general public,"[430] the statute makes it an offense to collect national defense information knowing that it may be published.[431] "National defense information" is defined slightly more narrowly than in S. 1, but does include:

[I]nformation, regardless of its origin, relating to:

(1) the military capability of the United States. . . .
* * * *
(5) military weaponry, weapons development, or weapons research of the United States. . . .
* * * *
(9) the conduct of foreign relations affecting the national defense. . . .[432]

Given the scope of "national defense information," the result would be to paralyze newspaper reporting on national defense affairs. We strongly doubt that the nation needs a far reaching official military secrets act. Surely it does not need one that makes the offense a capital crime when committed "during a national defense emergency" or when information concerns a "major weapons system or [a] major element of defense strategy,"[433] and a class B felony otherwise.[434]

Similarly, the rest of the offenses, with the exception of obtaining classified information,[435] are defined in terms so broad that they mark an abrupt departure from statutory precedents. Any knowing communication of defense information to an unauthorized person would be made a class C or D felony, and unauthorized retaining of defense information would be a class D felony, both without regard to any intention or knowledge respecting injury to the United States.[436] Disclosure of classified information by a present or former federal employee, except to a "regularly constituted" Congressional committee pursuant to "lawful demand," would be a Class E felony[437] and no defense that information was improperly classified would be permitted.[438]

The consequence of S. 1400's enactment would be to prohibit virtually all public and private speech about national defense secrets, leaving to prosecutors and juries to choose victims among those who engage in reporting and criticism of our defense and foreign policies. Like Senator Cummins in 1917, we can only marvel that legislation at once so sweeping and so stringent could be seriously proposed. We trust that it will not be enacted.

What should be done? In our reasonably open society, Congress and the newspapers reveal large amounts of defense information that would be difficult and exceedingly expensive for interested foreign governments to collect on their own. That form of foreign aid to adversaries is, however, a necessary consequence of the nation's deepest values.[439] We do not accord much significance to protests that as a general matter we make it easy for others to assess our strength[440] because our strength is so awesome. The more difficult questions concern the protection of secrecy in narrower premises where specific objectives, opportunities, and advantages are lost if particular types of secrets are publicized.[441] Unfortunately, to distinguish these matters—indeed to know whether they can effectively be distinguished—requires more knowledge than we have about intelligence affairs and the extent to which truly important security interests have been compromised by well-meant disclosures. We have nonetheless come to certain conclusions that, while general, may assist legislators and others in their consideration of the problems.

No legislation can be adequate unless it recognizes that at least three problems must be treated independently: spies, government employees and ex-employees, and newspapers and the rest of us.[442] Both the present espionage

430. *Id.* at § 1126(c).

431. It is difficult for us to believe that this was intended. It nonetheless is the technical result of the statute in that he who "obtains or collects" information "with knowledge" that it "may" be used to the advantage of a foreign power, and knowing that it "may be communicated to a foreign power" commits the highest offense.

432. S. 1400, 93d Cong., 1st Sess. § 1121, § 1126(g) (1971).

433. *See* § 2401(a)(1)(B). The death penalty is mandatory if the defendant "knowingly created a grave risk of substantial danger to the national security" and mitigating factors not likely to be present in publication are absent.

434. *Id.* at § 1121(b). Class B felonies are punishable by a maximum of 30 years imprisonment. § 2301(b)(2).

435. *Id.* at § 1125. It applies only to agents of [illegible] information which is, inter alia, defined, § 1126(b), as "information, regardless of its origin," which is marked by statute, or pursuant to executive order or implementing rules or regulations as "information requiring a specific degree of protection against unauthorized disclosure for reasons of national

436. *Id.* at §§ 1122(b), 1123(b). Class C felonies are punishable by a maximum of 15 years imprisonment § 2301(b)(3); class D felonies are punishable by a maximum of 7 years imprisonment, § 2301(b)(4).

437. *Id.* at § 1124(a)(c)(e). Class E felonies are punishable by a maximum of 3 years imprisonment § 2301(b)(5). How Congress can "demand" what it is ignorant of is left unexplained.

438. *Id.* at § 1124(d).

439. *Cf.* United States v. Robel, 389 U.S. 258, 264 (1967): "Implicit in the term 'national defense' is the notion of defending those values and ideals which set this Nation apart."

440. *See, e.g.*, A. DULLES, THE CRAFT OF INTELLIGENCE 241-247 (1963).

441. The archtypical case is revelation that a foreign code has been broken. Apparently, [illegible] prospect increasingly unlikely where sophisticated equipment may be used. For a fascinating discussion of code-breaking, see D. KAHN, THE CODEBREAKERS (1967).

442. Additionally, it may be wise to differentiate employees from ex-employees, and

statutes and the proposals of S. 1 and S. 1400[443] are fatally defective in that they ignore the necessity of separate considerations of the distinct interests in each of these contexts.

The essence of classical espionage is the individual's readiness to put his access to information of defense significance at the disposal of agents of foreign political organizations. Granted that the harm that results from his conduct is a function of the importance of the information transferred, there should be no hesitation, regardless of the banal quality of defense information involved, to punish the citizen whose priorities are so ordered or foreigners whose job it is to risk apprehension. We believe, therefore, that the information protected against clandestine transfer to foreign agents should be defined broadly, probably more broadly than in current law. In this context, we see no dispositive objection to making knowing and unauthorized transfer of classified information to foreign agents an offense, without regard to whether information is properly classified.[444] That a spy might earn complete immunity by stealing secrets so serious that their significance cannot be disclosed in court—a clear possibility under current law,[445] and also under S. 1 and S. 1400—is an outcome that should be avoided, if possible.

Two objections may be made to this broadened approach. First, it puts considerable reliance on the capacity to adjudicate accurately whether persons are in fact acting as agents of foreigners. If the prosecutor need not demonstrate the significance of the transferred information, there is an enhanced risk that casual disclosures of improperly classified information to foreign friends may be wrongly deemed espionage. Nothing in the literature, however, suggests to us that this is a serious problem, and it may be further minimized by insistence upon the actor's awareness that his disclosures are intended for primary use by foreign political organizations.[446] Second, and more troublesome to us, is the fact that for deterrence purposes the penalties for espionage are and should be exceptionally steep. Denying improper classification as a defense may expose an offender whose conduct has produced no real harm to the most serious penalties the law permits. To avoid this result the law might expressly authorize *in camera* sentencing proceedings, or, preferably to us, make the offense substantially less serious if the Government is unprepared to disclose the underlying significance of the material transferred.

Quite different issues are posed by revelations of defense secrets by government employees or ex-employees. Prohibiting employees from telling

443. In structure, S. 1400 is preferable to S. 1 in that it does differentiate government employment as a problem to be treated separately from espionage proper. Its failure is that it treats newspapers with a severity appropriate for spies.

444. We thus disagree with the analysis [illegible] COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, 454-55 (1970).

445. *See* text following note 124 *supra*.

446. If necessary, special protection for government servants authorized to negotiate with foreign governments might be created.

what they know at pain of criminal punishment obviously restricts the flow of information to the public and impairs the quality of public debate. Nonetheless, to say that any government employee or former employee is privileged to reveal anything he chooses at risk of sanctions no greater than dismissal accords too little weight to the need for security.

In our opinion some middle ground should be sought. Although statutes are no doubt exceptionally difficult to formulate, we think that the following principles provide appropriate guides to future legislative efforts. First, employee disclosures to Congress should be protected more rigorously than in S. 1400.[447] Second, no matter what information is protected against revelation, legislation should explicitly provide a justification defense, permitting the jury either to balance the information's defense significance against its importance for public understanding and debate, or to consider possible dereliction of duty by the employee's superiors.[448] To do otherwise would not recognize that the employee serves both the Government and the public.

Third, the information that is protected against employee revelation should be narrower than that protected against espionage. On this point we strongly disagree with S. 1400's drafting of simple disclosure proposals more broadly than espionage provisions, apparently on the misguided notion that since the penalties are less severe the conduct covered may be broader.[449] Our approach is the reverse: espionage has no claim to the law's sympathy and excessive severity is better cured by flexible grading of the offense than by narrow restriction of the information protected against transfer, which necessitate Government proof of defense significance. By contrast, informing the public of what the Government is doing is presumptively desirable. The hard problem is to find standards to define what limited information cannot be revealed to the public. Certainly the fact of classification should not be determinative since substantial overclassification is inevitable given the variety of inducements to official secrecy.[450] Improper classification must be a defense, and, if possible,

447. There are obviously exceedingly difficult issues to be resolved here, particularly insofar as revelation to a particular Senator or Congressman may be merely a conduit to public revelation immunized by congressional privilege, rather than a prelude to independent congressional investigation.

448. Any such defenses may result in lengthening trials and compromising security further. Nonetheless, there are clearly instances where broader duties to the public warrant the disclosure of defense information and where the issue would be confused by characterizing the problem as one of improper classification.

449. To be sure, the employee has obligations of loyalty, but so does the citizen contemplating espionage.

450. For recent reports on overclassification, see *Hearings on U.S. Government Information Policies and Practices—The Pentagon Papers—Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 1st Sess. pts. 1-3, 7 (1971) (Moorhead Hearings).

There are numerous possible treatments of the problem of overclassification, particularly automatic declassification of nearly everything after an arbitrary time period. For proposals, see ARCHIBALD, PROPOSED ALTERNATIVES TO THE PRESENT SYSTEM OF CLASSIFYING GOVERNMENT DOCUMENTS. *Id.* at 2293. Nonetheless, given that there are multiple reasons, some good and some bad, why Government officials want secrecy, we think substantial overclassification is inevitable

protected information should be defined even more narrowly and without direct reference to classification. Thus, even if the Constitution permits penalizing employee or ex-employee disclosure of any information that the Government is not legally obligated to reveal,[451] we think such a secretive position should be rejected as a matter of policy. Fourth, the offense of revealing protected information should be graded to respect the differences between loose talk and intentional efforts to compromise security.

Finally, there are the problems of the press and those who disclose defense information in the course of public and private discussion. The claim may be made that lines should be drawn in the same place as for government employees.[452] It may seem paradoxical to provide the press with the privilege of publishing the fruits of a crime, a result that inevitably occurs if more information is protected against employee disclosure than against publication. Nevertheless, it seems to us that an asymmetry of obligations between public servants and the rest of us should be preserved, at least until such time as far-reaching institutional changes are made in congressional access to defense information. Congress has no assured access to security information and no sense of entitlement to it, as the inability of the Foreign Relations Committee to secure the Pentagon Papers demonstrates.[453]

Consequently, one cannot at the present time have confidence that more than a single elected official, if that, has given consent to whatever policy may be compromised by newspaper disclosure of defense information. Given that situation, doubts whether to protect the political efficacy of disclosure rather than stress its adverse security consequences should be resolved on the side of public debate. Peacetime prohibition of newspaper disclosure and citizen communication should be left to the most narrowly drawn categories of defense information such as the technical design of secret weapons systems or information about cryptographic techniques. Even as to such narrow categories of defense-related information, however, it is as true today as it was in 1917 that any item of information could, in some circumstances, have significance for public debate which outweighs any adverse effect on national security. Thus, prohibitions against newspaper and citizen disclosure applicable only to very narrow categories of information should also provide for a justification defense turning on superceding importance for public debate.

The dangers endemic to the administration of such a justification defense should not be minimized. Juries may be inclined to accord weight to the respectability and influence of a media defendant in assessing the justification for publication of the particular defense information. Selective enforcement is a real danger. Moreover, predictability will largely be sacrificed with a resulting chill on publication that should be justifiable in the legal sense. But uncertainty in the application of legal standards to publication of defense information is the price of rejecting simplistic solutions to the problem. Neither prohibiting nor privileging the publication of categories of defense information across the board does justice to the vital and competing social interests in secrecy and public revelation.

We have lived throughout the present century with extraordinary confusion about the legal standards governing publication of defense information. Clarification of the standards is now called for. However, uncertainties in the administration of theoretically sound legislative solutions should not force us to choose between extreme and simplistic policies. If the choice is narrowed to extremes, we hope that our current lawmakers exhibit the fortitude of their predecessors in 1917 who resisted the sweeping proposals of the Wilson Administration.

451. *Cf.* Environmental Protection Agency v. Mink, 93 S. Ct. 827 (1973).

452. *Cf.* Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers* 120 U. PA. L. REV. 271, 278-79 (1971).

453. *See* S. UNGAR, *supra* note 3 at 69-71. Two intriguing aspects of the *New York Times* litigation were first, the Government's prompt concession in court that much of the material could be immediately declassified, and second, the claim that considerable time should be granted to winnow out the truly important information among that which was potentially sensitive. Both propositions provide insight on the seriousness with which Senator Fulbright's repeated requests were treated.

This is a central difference between the secrecy situation in Great Britain and our own. The British Official Secrets Act provides greater protection for Government secrecy than do our espionage laws. But in Great Britain, the persons with principal executive authority and access to secrets sit as elected officials, and their comments in Parliament are privileged, providing greater assurance against policies gone wild.

OGC 79-00075

Washington, D.C. 20505

4 JAN 1979

Honorable Edward P. Boland, Chairman
Permanent Select Committee on Intelligence
House of Representatives
Washington, D. C. 20515

Dear Mr. Chairman:

I am pleased to learn that your Committee will hold hearings in late January, 1979 on the use and protection of national security information in civil and criminal litigation. As you know, I testified before the Senate Select Committee on Intelligence about this subject in March of last year.

I firmly believe that your impending effort to address the problems surrounding the protection of legitimate national security secrets in the civil and criminal proceedings is both timely and necessary. As matters presently stand, the government's ability to protect its legitimate secrets is uncertain at best. As you know, that uncertainty exists in a variety of contexts, ranging from "leaks" by government employees to cases of espionage and the publication of books by former employees who had access to sensitive information. I am hopeful that your hearings will give sharper definition to these problems and will serve as the basis for sound policy and legislative judgments.

I am designating Mr. Anthony A. Lapham, my General Counsel, to appear as a witness at your hearings on my behalf.

Yours sincerely,

/s/ Stansfield Turner

STANSFIELD TURNER

OGC 79-00074

3 January 1979

MEMCRANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

FROM: Anthony A. Lapham
General Counsel

SUBJECT: ~~HPSCI Hearings on the Protection and Use of National Security Information in Criminal and Civil Litigation~~

1. ~~Action Requested: That you approve the recommendation in paragraph 5 and sign the letter to Chairman Boland at Tab D.~~

2. Background: Chairman Boland's letter to you of 22 December 1978 (Tab A) advises that the House Permanent Select Committee on Intelligence (HPSCI) will hold hearings in late January 1979 on the protection and use of national security information in criminal and civil litigation and asks that you designate witnesses to appear on your behalf to discuss problems the intelligence community has encountered in areas within the scope of the Committee's inquiry. Based on the Committee's statement of what it hopes to examine in the hearings (see "Prospectus," Tab B), the scope of the inquiry will be quite broad. While that scope includes some ground previously plowed by the SSCI, HPSCI intends to pick up where the Biden Subcommittee ended by examining, among other things, theories and specific proposals for amendment of the espionage laws and for making various unauthorized disclosures of classified information a crime, the legal theories for pre-publication review/restraint and post-publication remedies, the feasibility of special pre-trial procedures for national security cases, and, in closed session, why some actual espionage cases and damaging leaks were not investigated or prosecuted.

3. The above topics and other issues the HPSCI has identified will be a tall order for Congressman Morgan Murphy's Subcommittee on Legislation to tackle in just three and a half days of hearings. In addition to all of the above, HPSCI would like to hear from us on the recommendations contained in the Biden Subcommittee report. You have previously approved positions I suggested with respect to those recommendations (Tab C), so those positions should be the basis for our comments.

4. Staff Position: We have not yet had any discussion with the HPSCI staff on format and other aspects of the hearings. It is possible that we may need to obtain input from the Office of Security, the Special Security Center, and the DDO on some aspects, as for example the kinds of damage caused to intelligence interests by past leaks.

5. Recommendation: That you designate the undersigned as your principal witness for the hearings, with the understanding that I can call on other components and individuals to assist as needed, and that you sign the letter to Chairman Boland at Tab B.

STATINT

[redacted]

Anthony A. Lapham

Attachments

APPROVED:

4 JAN 1979

Director of Central Intelligence — Date

DISAPPROVED:

Director of Central Intelligence — Date

OGC 78-7377

3 November 1978

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

FROM: Anthony A. Lapham
General Counsel

SUBJECT: Report of the Senate Select Committee on Intelligence Subcommittee on Secrecy and Disclosure Entitled "National Security Secrets and the Administration of Justice"

1. Action Requested: None. This is for your information and consideration only.

2. Background: This memorandum relates to the subject report (Tab A), culminating over a year's study by the Subcommittee of the problems associated with the need to use classified information in criminal trials. You will recall that you testified before the Subcommittee in March of this year on the matter (your prepared statement is at Tab B).

3. In August, 1978 we received a draft of the Subcommittee's report which I felt was woefully deficient, pejorative, and misleading. I made my views known to Bill Miller, and at his request I put them in writing for the Subcommittee's consideration, (Tab C). The final version of the report was much improved, although the recommendations as they appeared in the draft were left virtually intact (see Tab D for a comparison of the recommendations in the draft and final versions of the report). What follows in this memorandum is a discussion of the report's recommendations, together with my views as to appropriatness of these recommendations and the position we should take on each.

First recommendation

4. The first recommendation states that Congress should focus on the development of statutory and administrative

ILLEG

procedures that would be designed to address the problems associated with discovery and use of classified information in criminal trials. The Subcommittee feels that, with one exception, such procedures, which are specifically outlined in the following recommendations, would be more useful than any attempted rewrite of the federal espionage statutes. The exception is the Subcommittee's endorsement of "limited" statutory protection for the identities of intelligence agents, sources and employees under cover. You have already proposed new legislation along these lines in your letter to the Attorney General of 17 August 1978, recommending amendment of 18 U.S.C. §798 to include classified information which identifies or tends to identify any CIA agent, source, or employee. Justice is currently studying your proposal as well as the broader subjects of sources and methods and leak legislation.

5. My own view is that an overhaul of the espionage laws is long overdue and that no amount of tinkering with existing procedures can compensate for the deficiencies of these laws. Therefore, while I think you should endorse the idea of improving the procedural rules governing the use of national security information in civil and criminal cases, and should welcome the Subcommittee's recognition that new legislation is needed to protect the identities of intelligence agency personnel, I do not think you should give your blessing to the idea of deferring a full-scale congressional reconsideration of the espionage laws.

Second recommendation

6. The second recommendation suggests that the executive branch interpret Executive Order 12065, the new classification order, in a way that will decrease unnecessary secrecy and declassify as many studies and reports as possible on matters of public concern in order to discourage the leaking of unsanitized documents and information. The recommendation emphasizes that declassification must be done in an objective manner. I am sure you have no quarrel with this recommendation. At the same time, however, the kind and amount of declassification contemplated by the Subcommittee is not likely to have much impact on the leak problem. In the first place, the substance of many past leaks would not be declassified under even a liberal declassification policy. This would be due in some cases to a source association problem and in others simply to sensitivity. Secondly, it would be virtually impossible to defuse all the subjects concerning which there may be a motive to leak for political or some other advantage. Therefore, while there is reason to endorse this recommendation, there is also reason to doubt that it represents much of a solution to the leak problem.

Third recommendation

7. Recommendation III proposes the following:

a. An administrative procedure (and system with attendant due process rights) for disciplining employees for security violations (probably contemplates a hearing and perhaps other procedural safeguards such as the right to be represented by counsel, to cross-examine witnesses, and to appeal);

b. Centralized authority, "perhaps in the IOB," for investigation of breach of security and violations that do not constitute crimes; and

c. Possible application of the administrative system to former employees, with penalties to include the loss of pension rights.

8. In my opinion this recommendation is largely without merit and should not be endorsed. The proposals in parts a. and b. would involve some shuffling of boxes, all to no good effect as I see it, and a new overlay of procedural requirements that if anything would make the problems more rather than less difficult. In the first place, there is no lack of authority now to discipline employees for security violations, and no need to establish a new system for doing so. In the second place, there is no apparent advantage in the idea of centralizing the responsibility for the investigation of leaks that do not constitute crimes, even if the distinction between criminal and non-criminal leaks were a matter of agreement, which it is not. Certainly the IOB could not perform the central investigating role envisioned by the Subcommittee without an expansion of its charter, in which case it would come to be seen as a new anti-leak bureaucracy rather than as an intelligence oversight body.

9. It would require legislation to implement part c. of this recommendation. The potential gains would be very small because, apart from the termination of an annuity, there is no effective administrative sanction that could be applied to former employees. Even termination of an annuity, however, would not be an effective remedy as to the likes of Agee, Snepp and Stockwell, none of whom is an annuitant. Moreover, Congress would be sure to surround the enforcement of such a remedy with an array of procedural rights, hearings, reviews, etc. All in all, I think we are better off to stick with secrecy agreements as the preferred non-criminal approach to the handling of security violations by former employees.

Fourth recommendation

10. This recommendation relates to the role of the FBI in the investigation of leaks. It is a mixed bag. On the one hand it proposes that, contrary to the existing Justice Department practice which has been a bone in our throat for so long, the FBI should undertake such investigations without advance agency commitments to declassify the information that might be needed for prosecution, and even though the outcome might be administrative action rather than prosecution. So far so good. It then goes on to propose that FBI investigations be limited to cases involving disclosure of intelligence information by officials, employees, or contractors having access to that information. If the unauthorized disclosure of classified information is a crime, which in my opinion is a highly doubtful proposition to begin with except where communications intelligence or cryptographic information is concerned, then the proposed limit on the FBI's investigative authority makes no sense. In addition, while recognizing that prosecution may not be the goal, the report proposes to limit the FBI's authority to cases involving criminal activity. Here again, however, the report makes no serious effort to distinguish between those leaks that are criminal under existing statutes and those that are not, and it is the uncertainty that prevails on this point that is at the root of the current dispute as to how best to deal with these matters. Moreover, the Justice Department has recently affirmed to us in a memorandum by John Harmon that the FBI has authority to investigate security violations in non-criminal contexts.

11. In sum, I would endorse this recommendation only insofar as it proposes an end to the current Justice Department policies, requiring up-front declassification decisions, which effectively preclude any FBI involvement in the investigation of leaks.

Fifth recommendation

12. Recommendation V calls for the Attorney General to issue guidelines pursuant to Executive Order 12036 for reporting by intelligence community agencies of all possible violations of U.S. law which come to the attention of such agencies. The recommendation states the guidelines "must consider the protection of sensitive sources and methods."

13. A requirement to report all possible violations of U.S. law would be broader than that currently contemplated and being developed pursuant to Section 1-706, E.O. 12036, at least insofar as it would pertain to non-employees. As you know that section calls for the reporting of all possible

violations of federal criminal law by employees and for reporting violations by other persons of such federal criminal laws "specified in guidelines adopted by the Attorney General." The language of Section 1-706 was phrased so as to retreat from the requirement imposed by E.O. 11905 that all possible violations by everyone be reported. The E.O. 11905 formulation gave us problems in connection with cover arrangements with corporations and other confidential relationships, which often provided us with knowledge of technical or minor violations of U.S. law. I touched on this problem when I appeared before Congressman Preyer's Subcommittee on Government Information and Individual Rights in September and pointed out that such a requirement is not imposed on any other agencies and would cause additional complications for our confidential relationships. There was no response to my statement by the Subcommittee.

14. The current efforts to develop guidelines under Section 1-706 for reporting federal crimes committed by non-employees are bogged down in the Department of Justice. Some of the offenses proposed for inclusion in the guidelines are still of concern to us, though I believe that any guidelines which narrow the reporting requirement to something less than all possible violations will be beneficial. I think you should support the current efforts under E.O. 12036 in this regard and reject the Subcommittee's suggestion that we be required to report all violations. I am hopeful that in the end we will be able to agree upon guidelines that will satisfy Congress, the Attorney General and the intelligence Community.

Sixth recommendation

15. Recommendation VI calls for the Attorney General to issue regulations that would establish procedures under which agencies of the IC would provide information to the Department of Justice necessary for the investigation or prosecution of a criminal case. In addition, the regulations would establish:

a. how the decision is made not to proceed in national security cases;

b. who could make the decision (which would be in writing); and

c. a requirement that there be a decision paper describing the intelligence information that would be disclosed in a trial, why it would be disclosed, and the damage it would cause if disclosed.

Finally the recommendation proposes that the required decision paper in such cases be available to the intelligence oversight committees of Congress and that the cases be reported annually or as required.

16. It is not altogether clear what the Subcommittee has in mind when it refers to regulations "binding upon all departments of the government" setting forth procedures to assure that necessary information would be made available to DOJ for purposes of criminal investigation or prosecution. You emphasized in your testimony before the Subcommittee that access by DOJ to relevant information is not and should not be an issue. However, if the intent is that the regulations should establish a right in DOJ to physical possession, control, and use of documents and files without consultation with or concurrence of the agencies concerned, then the proposal is objectionable. Your role in determining whether sensitive intelligence information should be used in a criminal investigation or trial is one that has been acknowledged by DOJ. On the other hand, if the intent is only to formalize DOJ rights of access to intelligence information, I do not see the need for a regulation and doubt that it could bind other departments in any event.

17. The proposal that the Attorney General adopt regulations to govern the dismissal of national security cases is one for DOJ to address, although my impression is that internal DOJ instructions already embody most of the requirements proposed by the Subcommittee. As for the idea of oversight committee review of these decisions, I am certain that DOJ would resist the idea and I do not think we should give it any encouragement.

Seventh recommendation

18. Recommendation VII proposes that Congress consider the adoption, presumably in the form of amendments to the Federal Rules of Criminal Procedure, of a special pre-trial procedure "to be used in cases where national secrets are likely to arise in the course of a criminal prosecution." The purpose of this procedure would be to "weed out" irrelevant defenses in advance of trial and to foreclose efforts to force the disclosure of national security information in support of such defenses, either during the discovery phase of a prosecution or at trial.

19. I am not attracted to the specifics of this proposal, in part because some of the suggested procedures are already available and in part because others would be clearly unworkable. But I certainly cannot say, in light of the recent experiences in the Berrellez and Kampiles cases, that there

is no room for procedural reform. On the contrary, I think, and my sense is that STATINTL either agrees or will soon agree, that it might be possible to develop a useful and workable proposal. Accordingly, I would endorse this recommendation in principle, reserving as to the particulars.

Eight recommendation

20. Recommendation VIII calls for Congress to reconsider adoption of the Supreme Court's proposed codification of a privilege for secrets of state. Without going into great detail, the Supreme Court's 1974 proposal defined a "secret of state" as a "governmental secret relating to the national defense or the international relations of the United States." The proposal would have allowed department and agency heads to claim the privilege in civil and criminal cases, after which the trial judge would determine in camera whether or not the privilege is justified. If the judge sustained the claim, the documents or statements in question would be sealed and unavailable to the defendant or other party. If sustaining the government's claim would deny the other party material evidence, the judge would have to determine an appropriate remedy, such as finding against the government on the issue to which the evidence is relevant, or dismissing the case.

21. The Subcommittee's recommendation embroiders on the Supreme Court's 1974 proposal, which encountered a storm of controversy and was dropped by the Congress. Among other things, the Subcommittee report apparently contemplates that the in camera proceedings would be adversary in nature, allowing for participation by defense counsel and perhaps even defendants. It is not evident to me how secrets could be protected under these arrangements. Nor is it evident to me that in most instances the judge would have any recourse except to dismiss the prosecution if he found that the privilege claim was valid and at the same time concluded that the information in question was relevant to the defense. Accordingly, I am very leery of this recommendation and would favor saying nothing more than that it deserves further consideration.

22. If you agree with the views I have set forth on the Subcommittee's recommendations, we will conduct our further discussions with the Subcommittee staff on this basis. STATIN

Anthony A. Lapham

cc: DDO
OGC:AAL:sin
1 - DDCI
1 - ER via Ex Secty
1 - OLC
1 - OGC